HKUST – Department of Computer Science and Engineering

COMP 2711: Discrete Math Tools for CS – Spring 2012

Midterm Examination 2

#

Date: Friday, April 13, 2012 Time: 19:00–21:00

Name: _____	Student ID: _____
Email: _____	Lecture and Tutorial: _____

Instructions

- This is a closed book exam. It consists of 13 pages and 8 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- **Unless otherwise specified you *must* always explain how you derived your answer. A number without an explanation will be considered an incorrect answer.**

Questions	1	2	3	4	5	6	7	8	Total
Points	14	14	15	10	8	13	13	13	100
Score									

Student ID: _____

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Student ID: _____

Problem 1: [14 points]
This problem is on the RSA algorithm for public key cryptorgraphy. To generate his keys, Bob starts by picking $p = 37$ and $q = 31$. So, $n = pq = 1147$ and $T = (p-1)(q-1) = 1080$.

(a) Bob's public key is a pair $(e, 1147)$. Which of the following integers can Bob use for e? Why?

(i) 17; (ii) 5; (iii) 49; (iv) 21.

(b) Suppose Bob chooses $e = 47$. Compute his private key d by running the extended GCD algorithm. Show all the steps.

Solution:

(a) (i), (iii). This is because they are the only ones that are relatively prime to T, that is, $gcd(e, T)$ must be 1. (ii) fails because 1080 and 5 are both divisible by 5. (iv) fails because 1080 and 21 are both divisable by 3.

(b) The private key should satisfy $(ed) \bmod T = 1$. i.e. d is multiplicative inverse of e in Z_T. Run the extended GCD algorithm to calculate it:

$$\begin{aligned} 1080 &= 47 \cdot 22 + 46 \\ 47 &= 46 \cdot 1 + 1 \end{aligned}$$

Then,

$$\begin{aligned} 1 &= 47 - 46 \\ &= 47 - (1080 - 47 \cdot 22) \\ &= 23 \cdot 47 + 1080 \cdot (-1) \end{aligned}$$

Thus, $d = 23$.

Grading:(a) 4 (1 point for each item, 0.5 for answer and 0.5 for explanation); (b) 10: only 2 if no steps are shown. Otherwise, deduct points for errors.

Student ID: _____

Problem 2: [14 points]
This problem is a continuation of Problem 1.

(a) Suppose Alice wants to send the message "964" to Bob. Compute the ciphertext for Alice using repeated squaring. Show all the steps.

(b) Suppose Bob gets the ciphertext "1086" from David. How does Bob decrypt the ciphertext to recover David's original message? Give the formula that **Bob** needs to use. There is **NO** need to recover the original message **yourself**.

Solution:

(a) The ciphertext $c = 964^{47} \bmod 1147 = 964^{(2^5+2^3+2^2+2^1+2^0)} \bmod 1147$. By the repeated squaring algorithm, we have

$$\begin{aligned}
I_0 &= 964^{2^0} \bmod 1147 = 964 \\
I_1 &= 964^{2^1} \bmod 1147 = (I_0 \cdot I_0) \bmod 1147 = 226 \\
I_2 &= 964^{2^2} \bmod 1147 = (I_1 \cdot I_1) \bmod 1147 = 608 \\
I_3 &= 964^{2^3} \bmod 1147 = (I_2 \cdot I_2) \bmod 1147 = 330 \\
I_4 &= 964^{2^4} \bmod 1147 = (I_3 \cdot I_3) \bmod 1147 = 1082 \\
I_5 &= 964^{2^5} \bmod 1147 = (I_4 \cdot I_4) \bmod 1147 = 784
\end{aligned}$$

Thus, $964^{(2^5+2^3+2^2+2^1+2^0)} \bmod 1147 = (964 \cdot 226 \cdot 608 \cdot 330 \cdot 784) \bmod 1147 = 642$.

(b) The original message $m = c^d \bmod n = 1086^{23} \bmod 1147$.

Grading: (a) 11 (3 for the formula, 8 for repeated squaring. Deduct points for errors); (b) 3

Student ID: _____

Problem 3: [15 points]
Consider the following modular equations:

$$\begin{aligned} x \bmod 11 &= 6 \\ x \bmod 13 &= 9 \\ x \bmod 15 &= 4 \end{aligned}$$

(a) Find an integer $x \in Z_{2145}$ that satisfies the equations. Note that $2145 = 11 \times 13 \times 15$. For this question, there is **no** need to show the steps of the extended GCD alogrithm.

(b) Prove by contradiction that the solution is unique.

Solution:

(a) By the extended GCD algorithm, we have $(11 \cdot 13) \cdot 2 \bmod 15 = 1$, $(11 \cdot 15) \cdot 3 \bmod 13 = 1$, $(13 \cdot 15) \cdot 7 \bmod 11 = 1$. Set $y = 6 \cdot 13 \cdot 15 \cdot 7 + 9 \cdot 11 \cdot 15 \cdot 3 + 4 \cdot 11 \cdot 13 \cdot 2$ satisfies the equations. The final answer $x \in Z_{2145}$ is $x = y \bmod 2145 = 919$.

(b) Suppose that the solution is not unique. Then, there are two values $x', x \in Z_{2145}$ that satisfy the given equations, and we have the following:

$$\begin{aligned} x \bmod 11 &= 6 \Rightarrow (x-6) = a11 \Rightarrow (x - a11) = 6 \\ x' \bmod 11 &= 6 \Rightarrow (x'-6) = a'11 \Rightarrow (x' - a'11) = 6 \\ x \bmod 13 &= 9 \Rightarrow (x-9) = b13 \Rightarrow (x - b13) = 9 \\ x' \bmod 13 &= 9 \Rightarrow (x'-9) = b'13 \Rightarrow (x' - b'13) = 9 \\ x \bmod 15 &= 4 \Rightarrow (x-4) = c15 \Rightarrow (x' - c15) = 4 \\ x' \bmod 15 &= 4 \Rightarrow (x'-4) = c'15 \Rightarrow (x' - c'15) = 4 \end{aligned}$$

where a, a', b, b', c, c' are integers, and $a \neq a', b \neq b', c \neq c'$. Combining the above, we have:

$$\begin{aligned} (x - a11) = (x' - a'11) &\Rightarrow (x - x') = (a - a')11 \\ (x - b13) = (x' - b'13) &\Rightarrow (x - x') = (b - b')13 \\ (x - c15) = (x' - c'15) &\Rightarrow (x - x') = (c - c')15 \end{aligned}$$

This means that *all* $\{11, 13, 15, (a - a'), (b - b'), (c - c')\}$ *divide* $(x - x')$. Let f be the prime factorization of $|x - x'|$. Then, product $11 \cdot 13 \cdot 15$ must appear in f. Consequently, $|x - x'| \geq 11 \times 13 \times 15 = 2145$. However, due to the fact that $x, x' \in Z_{2145}$, $0 \leq |x - x'| < 2145$. Therefore, we reach a contradiction, which means that the solution must be unique.

Grading: (a) 7; (b) 8. Most students will not get this part. Find reasons to give points.

Student ID: _____

Problem 4: [10 points] Let p be a prime number (and hence $p \geq 2$).

(a) Show that there are $p^2 - p$ elements with multiplicative inverses in Z_{p^2}.

(b) If x has no multiplicative inverse in Z_{p^2}, what is $x^{p^2-p} \bmod p^2$? Explain your answer.

Solution:

(a) The numbers $0, p, 2p, 3p, \ldots, (p-1)p$ have no multiplicative inverses since they are not relatively prime to p^2. But other elements in Z_{p^2} have a multiplicative inverse because they have no factor p and thus they are relatively prime to p^2. So, there are $p^2 - p$ elements with multiplicative inverse in Z_{p^2}.

(b) For any element x with no multiplicative inverse, we can write $x = qp$, where q is an integer and $0 \leq q < p$. So, $x^{p^2-p} = (qp)^{p^2-p} = q^{p^2-p} \cdot p^{p^2-p} = (p^2(q^{p^2-p} \cdot p^{p^2-p-2}))$ which is multiple of p^2, since $p^2 - p \geq 2 \Rightarrow p^2 - p - 2 \geq 0$ for any prime p. Thus, $x^{p^2-p} \bmod p^2 = (p^2(q^{p^2-p} \cdot p^{p^2-p-2})) \bmod p^2 = 0$.

Grading: 5 points each.

Student ID: _____

Problem 5: [8 points]
This question is on logic. You may give your answers without explanations.

(a) Convert the logic statement $\neg(p \Rightarrow \neg q)$ to an equivalent statement that involves only the AND ($\wedge$) connective.

(b) Convert the logic statement $(p \vee q) \wedge r$ to an equivalent statement that involves only the $IMPLY$ ($\Rightarrow$) and NOT ($\neg$) connectives.

(c) Convert the logic statement $(((p \vee q) \vee \neg(p \vee q)) \Rightarrow r) \vee s$ to an equivalent statement that involves only the OR ($\vee$) connective.

Solution:

(a) $\neg(p \Rightarrow \neg q) \equiv \neg(\neg p \vee \neg q) \equiv (p \wedge q)$.

(b) $(p \vee q) \wedge r \equiv (\neg p \Rightarrow q) \wedge r \equiv \neg(\neg(\neg p \Rightarrow q) \vee \neg r) \equiv \neg((\neg p \Rightarrow q) \Rightarrow \neg r)$.

(c) $(((p \vee q) \vee \neg(p \vee q)) \Rightarrow r) \vee s \equiv (True \Rightarrow r) \vee s \equiv r \vee s$

Grading: 2, 3, 3

Student ID: _____

Problem 6: [13 points]
A logic statement is in **prenex normal form (PNF)** if and only if it is of the form

$$Q_1 x_1 \, (Q_2 x_2 \, \ldots \, (Q_n x_n \, (P(x_1, x_2, \ldots, x_n))) \ldots)$$

where each Q_i for $i = 1, 2, \ldots, n$ is either the existential or the universal quantifier, and $P(x_1, x_2, \ldots, x_n)$ is a logic statement on the variables $x_1, x_2, \ldots, x_n$ that involves no quantifiers. For example, $\exists x \, (\forall y \, (p(x, y) \wedge q(y)))$ is in PNF, whereas $\exists x \, (p(x)) \vee \forall y \, (q(y))$ is not in PNF.

Convert the following logic statements into PNF. You may just write your answer, without explanation.

(a) $\exists x \, (p(x)) \vee \exists x \, (q(x))$.

(b) $\forall x \, (p(x)) \vee \exists x \, (q(x))$.

(c) $\exists x \, (p(x)) \Rightarrow \exists x \, (q(x))$

Solution:

(a) $\exists x \, (p(x) \vee q(x))$

(b) $\forall x \, (\exists y \, (p(x) \vee q(y)))$ We need the y in order to write the quantification correctly.

(c) First, we need to do some work. It holds that $\exists x \, (p(x)) \Rightarrow \exists x \, (q(x))$ is equivalent to $\neg \exists x \, (p(x)) \vee \exists x \, (q(x))$. This is further equivalent to $\forall x \, (\neg p(x)) \vee \exists x \, (q(x))$. Finally, because of (b), it holds that

$$\forall x \, (\exists y \, (\neg p(x) \vee q(y)))$$

.

Grading: 4, 4, 5

Student ID: _____

Problem 7: [13 points]
Let m be a nonnegative integer and n be a positive integer. Prove by induction that there exist integers q, r such that

$$m = nq + r, \text{ with } 0 \leq r < n.$$

Note that in class we have proved this by smallest counter-example.

Solution: Base Case: $m = 0$
If $m = 0$, then we can take $q = 0$ and $r = 0$. It is clear that $0 \leq r < n$ and $m = 0 = 0q + 0 = 0$. So the proposition is true when $m = 0$.

Inductive Step:
Suppose the proposition is true for m, i.e., there exist integers q, r such that

$$m = nq + r, \text{ with } 0 \leq r < n. \tag{1}$$

Now consider the case of $m + 1$. In Equation (1), we have $0 \leq r < n$. We break up this into two cases:

(1) $0 \leq r < n - 1$:
Because $m = nq + r$, we have $m + 1 = nq + r + 1$. Let $r' = r + 1$, then we have

$$m + 1 = nq + r', \text{ with } 0 \leq r' < n.$$

(2) $r = n - 1$:
Because $m = nq + r$, we have $m + 1 = nq + r + 1 = n(q + 1)$. Let $q' = q + 1$ and $r' = 0$, then we have

$$m + 1 = nq' + r', \text{ with } 0 \leq r' < n.$$

Thus by induction we have proved this proposition.
Grading: Most students should get this right. Deduct points for errors.

Student ID: _____

Problem 8: [13 points]
Let n be a positive integer such that $n > 1$. Give a contrapositive proof that if $2^n - 1$ is prime, then n must be prime.

Solution: The contraposition is:

If n is not prime, then $2^n - 1$ is composite.

Because n is not prime, then $n = p * q$, for integers $p, q > 1$. Then,

$$2^n - 1 = (2^p)^q - 1 = (2^p - 1) * ((2^p)^{(q-1)} + (2^p)^{(q-2)} + ... + (2^p) + 1)$$

Note that $2^p - 1 > 1$. Also, $(2^p)^{(q-1)} + (2^p)^{(q-2)} + ... + (2^p) + 1 > 1$. So we have factored $2^n - 1$, thus it is not prime.

We have proved the contraposition. So the original statement is true.

Grading: 4 points for stating the contraposition; 9 points for the rest. Most students will not get this. Find reasons to give points.

Student ID: _____

Scrap Paper

Student ID: _____

Scrap Paper

Student ID: _____

Scrap Paper